PCT/JP2005/002110

日本国特許庁 07. 2. 2005
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月　９日

出願番号
Application Number: 特願２００４－０３２６７６
[ST. 10/C]: [ＪＰ２００４－０３２６７６]

出願人
Applicant(s): 松下電器産業株式会社

２００５年　３月１０日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

BEST AVAILABLE COPY

出証番号　出証特２００５－３０２０４４９

【書類名】　特許願
【整理番号】　2048150058
【あて先】　特許庁長官殿
【国際特許分類】　G06F
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　原田　俊治
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山本　雅哉
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　岡本　隆一
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
【手数料の表示】
　【予納台帳番号】　049515
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0213583

【書類名】特許請求の範囲
【請求項１】
デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理装置であって、安全にデータ制御を行うデータ制御手段と安全にデータの記憶を可能とする記憶手段とを備え、
前記データ制御手段は、
秘密鍵を保持する秘密鍵保持部と、
前記秘密鍵でライセンス情報を暗号化する暗号化部と、
前記暗号化されたライセンス情報を前記記憶手段に移管する移管部とを備える
ことを特徴とするライセンス情報管理装置。
【請求項２】
前記データ制御手段は、さらに、
前記記憶手段から暗号化されたライセンス情報を読み出す読出部と、
前記読み出されたライセンス情報を復号する復号部と、
デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新部と、
前記更新されたライセンス情報を暗号化して、前記記憶手段に上書きする上書部とを備える
ことを特徴とする請求項１記載のライセンス情報管理装置。
【請求項３】
前記記憶手段は、さらに、
前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部を備え、
前記データ制御手段は、さらに、
前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部と、
前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証部を備える
ことを特徴とする請求項２記載のライセンス情報管理装置。
【請求項４】
前記更新履歴を表わす情報は、
アップデート回数又は乱数を表わす情報である
ことを特徴とする請求項３記載のライセンス情報管理装置。
【請求項５】
前記デジタルコンテンツは暗号化されており、
前記ライセンス情報は、
前記デジタルコンテンツの利用可能な範囲を示す条件を規定する再生条件情報と前記デジタルコンテンツを復号するためのコンテンツ鍵とを含む
ことを特徴とする請求項１～４記載のライセンス情報管理装置。
【請求項６】
デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理方法であって、
前記ライセンス情報管理方法は、
安全にデータ制御を行うデータ制御ステップを有し、
前記データ制御ステップは、
秘密鍵を保持する秘密鍵保持サブステップと、
前記秘密鍵でライセンス情報を暗号化する暗号化サブステップと、
前記暗号化されたライセンス情報を安全にデータの記憶を可能とする記憶手段に移管する移管サブステップとを含む

ことを特徴とするライセンス情報管理方法。
【請求項７】
前記データ制御ステップは、さらに、
前記記憶手段から暗号化されたライセンス情報を読み出す読出サブステップと、
前記読み出されたライセンス情報を復号する復号サブステップと、
デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新サブステップと、
前記更新されたライセンス情報を暗号化して、前記記憶手段に上書きする上書サブステップとを含む
ことを特徴とする請求項６記載のライセンス情報管理方法。
【請求項８】
前記記憶手段は、さらに、
前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部と、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部とを備え、
前記データ制御ステップは、さらに、
前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証サブステップを含む
ことを特徴とする請求項７記載のライセンス情報管理方法。
【請求項９】
デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理装置のためのプログラムであって、
前記プログラムは、
安全にデータ制御を行うデータ制御ステップを有し、
前記データ制御ステップは、
秘密鍵を保持する秘密鍵保持サブステップと、
前記秘密鍵でライセンス情報を暗号化する暗号化サブステップと、
前記暗号化されたライセンス情報を安全にデータの記憶を可能とする記憶手段に移管する移管サブステップとを
コンピュータに実行させることを特徴とするプログラム。
【請求項１０】
前記データ制御ステップは、さらに、
前記記憶手段から暗号化されたライセンス情報を読み出す読出サブステップと、
前記読み出されたライセンス情報を復号する復号サブステップと、
デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新サブステップと、
前記更新されたライセンス情報を暗号化して　前記記憶手段に上書きする上書サブステップとを含む
ことを特徴とする請求項９記載のプログラム。
【請求項１１】
前記記憶手段は、さらに、
前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部と、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部とを備え、
前記データ制御ステップは、さらに、
前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証サブステップを含む
ことを特徴とする請求項１０記載のプログラム。

【書類名】明細書
【発明の名称】ライセンス情報管理装置およびライセンス情報管理方法
【技術分野】
【０００１】
本発明は、暗号化されているデジタルコンテンツ等を再生する際の鍵情報や再生条件などを規定したライセンス情報の管理装置及びその管理方法に関し、特に、耐タンパ性を確保しながら上記ライセンス情報を管理する技術に関する。
【背景技術】
【０００２】
近年、ブロードバンド等のネットワークを利用したコンテンツ（例えば、映像、音声、プログラムソフトなど）配信が普及している。さらに、ＢＤ－ＲＯＭ(Blue ray Disc－Read Only Memory)パッケージを用いたコンテンツ配信の検討も進んでいる。一般に、これらのコンテンツには暗号化が施されているため、ユーザは、コンテンツに対応する復号鍵を入手する必要がある。さらに、上記コンテンツは、料金の支払いを前提とした利用制限が課されている場合が多く、ユーザは、所定のライセンス情報（例えば、ライセンスチケット）に従ってコンテンツを利用することとなる。ここで、「ライセンスチケット」とは、コンテンツの利用を制限するための条件を規定した情報である「コンテンツ再生条件情報」と、受信したコンテンツを復号するための鍵である、暗号化されている「コンテンツ鍵」とを含む情報をいう。この「コンテンツ再生条件情報」は、例えば、再生可能な日時について規定したり、再生可能な総時間について規定したり、再生可能な回数について規定したりするための情報である。
【０００３】
このため、ライセンスチケットについては厳重な管理が要求され、一般に、ライセンスチケットは、許可が認められないと書換えができない領域（耐タンパ領域）に保持される（例えば、特許文献１参照）。
図９は、従来の技術に係るコンテンツ再生装置５００の機能構成を示すブロック図である。コンテンツ再生装置５００は、暗号化されたコンテンツ（例えば、ＢＳデジタル放送の場合であれば、コンテンツの暗号化には、スクランブル鍵、ワーク鍵及びマスタ鍵が使用される。）を再生（利用）する際に必要となるライセンスチケットを耐タンパ性を確保しながら管理する装置であり、耐タンパモジュール部（以下「ＴＲＭ(Tamper Resistance Module)部」と記す。）５１０、コンテンツ復号部５２０、デコード部５３０及び操作入力部５３５を備える。なお、コンテンツ再生装置５００は、他に外部のネットワークに接続してデータの送受信を制御する通信制御部等を備えてもよい。
【０００４】
ＴＲＭ部５１０は、例えば耐タンパ性を有するＩＣカードで構成され、上記ライセンスチケットの管理を行う部署であり、コンテンツ再生条件情報５１１ａと暗号化されたコンテンツ鍵５１１ｂを格納するライセンスチケット格納部５１１、コンテンツ再生条件情報５１１ａに基づいてコンテンツの再生を制御するコンテンツ再生条件管理部５１２、ＴＲＭ部５１０で使用する固有鍵等を格納するＴＲＭ固有鍵格納部５１３、及びＴＲＭ固有鍵を用いてコンテンツ鍵の復号を行うコンテンツ鍵復号部５１４を備える。
【０００５】
コンテンツ復号部５２０は、コンテンツ鍵復号部５１４において復号されたコンテンツ鍵を用いて暗号化されたコンテンツ５５０の復号を行う。
デコード部５３０は、コンテンツ復号部５２０において復号されたコンテンツをディスプレイ５４０が表示可能なデータにデコードする。操作入力部５３５は、例えばスイッチやリモコン等であり、ユーザから「再生」などの操作を受け付けて、コンテンツ復号部５２０やコンテンツ再生条件管理部５１２に通知する。
【０００６】
コンテンツンツ再生装置５００の動作は、以下の通りである。
最初に、センタ６００から入手されたＴＲＭ部５１０（ＩＣカード）がコンテンツ再生

装置５００のカード挿入口等（図示せず）に挿入され、操作入力部５３５を介してユーザから再生指示を受け付けると、コンテンツ再生条件管理部５１２は、再生指示の対象となったコンテンツを特定し、ライセンスチケット格納部５１１から、上記コンテンツに対応するライセンスチケットのコンテンツ再生条件情報５１１ａを特定して、その内容を解読する。さらに、コンテンツ再生条件管理部５１２は、コンテンツ再生条件情報５１１ａの内容がコンテンツの再生を許可し得る条件であるか否かを判定し、再生が可能な場合は、ライセンスチケット格納部５１１に格納されている暗号化されたコンテンツ鍵５１１ｂを読み出してコンテンツ鍵復号部５１４に送信する。コンテンツ鍵復号部５１４は、ＴＲＭ固有鍵格納部５１３からＴＲＭ固有鍵を読み出し、暗号化されたコンテンツ鍵５１１ｂを復号し、これをコンテンツ復号部５２０に送信する。コンテンツ復号部５２０は、コンテンツ鍵復号部５１４から受信した、復号されたコンテンツ鍵に基づいて上記コンテンツを復号し、復号したコンテンツをデコード部５３０に送信する。

【０００７】

さらに、コンテンツ復号部５２０は、コンテンツの再生に関する情報（例えば、コンテンツ名、再生開始日時、再生終了日時など）をコンテンツ再生条件管理部５１２に送信する。これにより、コンテンツ再生条件管理部５１２は、再生されたコンテンツに対応するコンテンツ再生条件情報５１１ａの内容を変更し、ライセンスチケット格納部５１１に上書きする。なお、上記のコンテンツ鍵復号部５１４とコンテンツ復号部５２０間は、ＳＡＣ(Secure Authentication Channel：認証付きの安全な通信路)で結ばれている。

【０００８】

以上のように、コンテンツ再生装置５００は、再生条件情報であるライセンスチケットを耐タンパ性を確保しながら管理している。

【特許文献１】特開平０１－１９４０２９号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

しかしながら、上記ライセンスチケットについては、利用料配分などを容易にするために「１コンテンツ１ライセンスチケット」という形態をとっており、１ユーザが多数のコンテンツを所有する場合は、これに応じてライセンスチケットの数も多くなり、ライセンスチケットを格納するためのメモリ容量も増大する。このため、大容量のＴＲＭ部が必要となり、コンテンツ再生装置のコスト増につながり、最終的には競争力の低下の原因となる。

【００１０】

そこで、本発明は、ユーザが多数のコンテンツを所有する場合であっても、大容量のＴＲＭ部が必要とならないライセンス情報管理装置及びライセンス情報管理方法を提供することを目的とする。

【課題を解決するための手段】

【００１１】

上記の目的を達成するために、本発明に係るライセンス情報管理装置は、デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理装置であって、安全にデータ制御を行うデータ制御手段と安全にデータの記憶を可能とする記憶手段とを備え、前記データ制御手段は、秘密鍵を保持する秘密鍵保持部と、前記秘密鍵でライセンス情報を暗号化する暗号化部と、前記暗号化されたライセンス情報を前記記憶手段に移管する移管部とを備える。

【００１２】

これにより、従来ＴＲＭ部（耐タンパ性を有するＩＣカード）に格納していたライセンスチケットをセキュアフラッシュ部に格納することとしたので、ＴＲＭ部における記憶容量を最小限に抑えることが可能となる。

また、本発明に係るライセンス情報管理装置の前記データ制御手段は、さらに、前記記憶手段から暗号化されたライセンス情報を読み出す読出部と、前記読み出されたライセン

ス情報を復号する復号部と、デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新部と、前記更新されたライセンス情報を暗号化して、前記記憶手段に上書きする上書部とを備えてもよい。

【００１３】

さらに、本発明に係るライセンス情報管理装置の前記記憶手段は、さらに、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部を備え、前記データ制御手段は、さらに、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部と、前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証部を備えるように構成することもできる。

【００１４】

これにより、ライセンスチケットをセキュアフラッシュ部に格納すると共に、ライセンスチケットを識別し得る情報（ＬＴ＿ＩＤ）とアップデート回数とが対応付けられている対応表に基づいてライセンスチケットの正当性も検証するので、ＴＲＭ部の記憶容量を最小限に抑えると共に、より安全性を高めてライセンスチケットを管理することが可能となる。

【００１５】

なお、本発明は、上記ライセンス情報管理装置における特徴的な構成手段をステップとするライセンス情報管理方法として実現したり、それらステップをパーソナルコンピュータ等に実行させるプログラムとして実現したりすることもできる。そして、そのプログラムをＤＶＤ等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは云うまでもない。

【発明の効果】

【００１６】

以上の説明から明らかなように、本発明によれば、従来ＴＲＭ部（耐タンパ性を有するＩＣカード）に格納していたライセンスチケットをセキュアフラッシュ部に格納することとしたので、ＴＲＭ部における記憶容量を最小限に抑えることが可能となる。

さらに、本発明によれば、ライセンスチケットをセキュアフラッシュ部に格納すると共に、ライセンスチケットを識別し得る情報（ＬＴ＿ＩＤ）とアップデート回数とが対応付けられている対応表に基づいてライセンスチケットの正当性も検証するので、ＴＲＭ部の記憶容量を最小限に抑えると共に、より安全性を高めてライセンスチケットを管理することが可能となる。

ことができる。

【００１７】

従って、デジタル放送やパッケージソフト、ネットワーク等を介してデジタル著作物の流通や配信等が活発になり、適切な著作権保護の要請が高い今日においては、本願発明の~~実用的無価~~は極めて高い。

【発明を実施するための最良の形態】

【００１８】

以下、本発明に係る実施の形態について、図面を参照しながら詳細に説明する。

（実施の形態１）

図１は、本実施の形態に係るコンテンツ再生装置１００の機能構成を示すブロック図である。図１のコンテンツ再生装置１００は、暗号化されたコンテンツを再生（利用）する際に必要となるライセンスチケット（以下において、「ＬＴ(License Ticket)」とも記す。）を耐タンパ性を確保しながら管理する装置であり、ＴＲＭ部１１０、セキュアフラッシュ部１２０、コンテンツ復号部５２０、デコード部５３０及び操作入力部５３５を備える。なお、コンテンツ再生装置１００は、他に外部のネットワークに接続してデータの送受信を制御する通信制御部（図示せず）等を備えてもよい。

【００１９】

なお、本コンテンツ再生装置１００においては、上記従来技術のコンテンツ再生装置５００と同一の機能構成については同一の符番を付し、その説明は省略することとする。

ＴＲＭ部１１０は、例えば、耐タンパ性を有するＩＣカードであり、コンテンツ再生条件管理部１１１、ＴＲＭ固有鍵格納部５１３及びコンテンツ鍵復号部５１４を備える。

コンテンツ再生条件管理部１１１は、ＴＲＭ部１１０全体の制御を行う部署であり、センタ６００を介して入手した、暗号化されたコンテンツ５５０に対応するライセンスチケットを暗号化してセキュアフラッシュ部１２０に格納すると共に、ユーザによってコンテンツが再生される毎に、そのコンテンツに対応するコンテンツ再生条件情報５１１ａの更新を行う部署である。

【００２０】

セキュアフラッシュ部１２０は、例えば汎用のフラッシュメモリであるが、暗号化されたコンテンツ５５０に対応するライセンスチケット（即ち、コンテンツ再生条件情報５１１ａ及び暗号化されたコンテンツ鍵５１１ｂ）の書き込み／読み出しの際には、ＴＲＭ固有鍵によって暗号化／復号化が行われるという特徴を有している。具体的には、コンテンツ再生条件管理部１１１が、ＴＲＭ固有鍵格納部５１３に格納されているＴＲＭ固有鍵を用いて、セキュアフラッシュ部１２０から読み出されたライセンスチケットの復号を行う。また、ＴＲＭ固有鍵を用いて、更新されたライセンスチケットを暗号化し、これをセキュアフラッシュ部１２０に書き込む。

【００２１】

図２は、上記コンテンツ再生条件管理部１１１の機能構成を示すブロック図である。図２に示されるように、コンテンツ再生条件管理部１１１は、再生状況分析部１１２、全体制御部１１３及び暗号化／復号化部１１４を備える。

再生状況分析部１１２は、コンテンツの再生に関する情報（例えば、コンテンツ名、再生開始日時、再生終了日時など）をコンテンツ復号部５２０から受信すると、これらの情報に基づいてコンテンツの再生状況を表す情報である再生状況情報（例えば、コンテンツ名に対応する再生回数、再生日、再生総時間等）を生成し、これを全体制御部１１３に通知する。

【００２２】

全体制御部１１３は、コンテンツ再生条件管理部１１１の全体を制御する部署であり、例えばＲＯＭやＲＡＭを備えるマイクロコンピュータである。全体制御部１１３は、再生状況分析部１１２から受信した上記再生状況情報に基づいて、暗号化／復号化部１１４を介して読み出したコンテンツ再生条件情報５１１ａの更新を行い、これを暗号化してセキュアフラッシュ部１２０に上書きするように暗号化／復号化部１１４に指示する。さらに、全体制御部１１３は、必要に応じてＴＲＭ固有鍵格納部５１３に格納されているＴＲＭ固有鍵を読み出し、これを暗号化／復号化部１１４及びコンテンツ鍵復号部５１４に送信する。さらにまた、全体制御部１１３は、暗号化／復号化部１１４における暗号化処理又は復号化処理のタイミングを制御する。

【００２３】

また、全体制御部１１３は、ＩＣカードがカード挿入口に挿入され、新たにライセンスチケットが購入されたことを検知すると、一旦内部のＲＡＭ等に格納し、その後、このライセンスチケットをセキュアフラッシュ部１２０に移動（即ち、新規なライセンスチケットをセキュアフラッシュ部１２０に格納し、ＩＣカード内のライセンスチケットを削除）する。

【００２４】

なお、上記のように、ＩＣカードがカード挿入口に挿入されことを検知して新たに購入されたライセンスチケットをセキュアフラッシュ部１２０に移動する方法に限らず、上記通信制御部（図示せず）を利用してライセンスチケットを入手し、これを全体制御部１１３が検知してセキュアフラッシュ部１２０に移動するように構成してもよい。

暗号化／復号化部１１４は、全体制御部１１３の指示に基づいて、セキュアフラッシュ部１２０に対するコンテンツ再生条件情報５１１ａの読み出しと復号化処理、又は暗号化

処理と書き込みを行う。

【００２５】

図３は、上記図２に示したコンテンツ再生条件管理部１１１における処理の流れを示すフローチャートである。

最初に、全体制御部１１３は、コンテンツ復号部５２０及び操作入力部５３５を介して、ユーザからコンテンツの再生指示を受け付けた旨を受信すると（Ｓ２０１：Ｙｅｓ）、当該再生指示に対応するコンテンツを特定する（Ｓ２０２）。

【００２６】

次に、全体制御部１１３は、特定されたコンテンツに対応するライセンスチケットが存在する（即ち、ライセンスチケットが購入されている）か否かを確認し（Ｓ２０３）、確認できた場合は、上記従来の技術の場合と同様に、コンテンツ鍵を復号してコンテンツ復号部５２０に送信する。

上記のライセンスチケットの存否を確認する方法としては、例えば、新規に購入されたライセンスチケットをセキュアフラッシュ部１２０に移動する際に、当該ライセンスチケットを識別し得る情報（例えば、ライセンスチケットのＩＤ、以下「ＬＴ＿ＩＤ」と略称する。）を全体制御部１１３内のＲＡＭに保持しておき、上記再生指示を受け付けた際に、そのコンテンツに対応するＬＴ＿ＩＤが全体制御部１１３内のＲＡＭに存在するか否かを確認する。もし、対応するライセンスチケットが存在しない場合（Ｓ２０３：Ｎｏ）、全体制御部１１３は、エラー処理を実行する（Ｓ２０８）。

【００２７】

その後、全体制御部１１３は、コンテンツ復号部５２０からコンテンツの再生に関する情報を受信すると（Ｓ２０４：Ｙｅｓ）、ＴＲＭ固有鍵格納部５１３に格納されているＴＲＭ固有鍵を用いてセキュアフラッシュ部１２０に格納されているライセンスチケットを復号するように暗号化／復号化部１１４に指示する（Ｓ２０５）。

さらに、全体制御部１１３は、復号されたライセンスチケットのコンテンツ再生条件情報５１１ａの内容を更新して、再び上記ＴＲＭ固有鍵を用いて暗号化するように、暗号化／復号化部１１４に指示する（Ｓ２０６）。これにより、暗号化／復号化部１１４は、更新されたライセンスチケットを暗号化してセキュアフラッシュ部１２０に上書きする（Ｓ２０７）。

【００２８】

以上のように、本実施の形態に係るコンテンツ再生装置によれば、従来ＴＲＭ部（耐タンパ性を有するＩＣカード）に格納していたライセンスチケットをセキュアフラッシュ部に格納することとしたので、ＴＲＭ部における記憶容量を最小限に抑えることが可能となる。

【００２９】

（実施の形態２）

上記実施の形態１においては、コンテンツに対応するライセンスチケットをセキュアフラッシュ部に格納して、ＴＲＭ部の記憶容量の増大を回避する実施例について説明したが、本実施の形態では、さらに、セキュアフラッシュ部に格納されているライセンスチケットが、不正に書き換えられてしまうことを防止する実施例について説明する。

【００３０】

図４は、セキュアフラッシュ部に格納されているライセンスチケットが不正に書き換えられてしまう様子を説明するための図である。図４に示されるように、例えば、あるコンテンツについては、最大「１０時間」の再生を認めるようにライセンスチケットが設定されている場合に、５時間再生した場合、残りの再生可能時間は「５時間」の筈である。しかし、セキュアフラッシュ部１２０は、汎用のメモリであるため、任意に読出し／書き込みが可能であり、再生前の「１０時間」を示すライセンスチケットのデータを他のメモリ領域に事前にコピーしておき、コンテンツを５時間再生した後に、再び「１０時間」を示す古いライセンスチケットのデータを上書きすることが可能である。

【００３１】

そこで、本実施の形態では、ＴＲＭ部内にＬＴ＿ＩＤとライセンスチケットのアップデート回数の対応表を保持し、この対応表に基づいて、上記の不正を防止するコンテンツ再生装置について説明する。

図５は、本実施の形態に係るコンテンツ再生装置２００の機能構成を示すブロック図である。なお、本コンテンツ再生装置２００においては、上記実施の形態１のコンテンツ再生装置１００と同一の機能構成については同一の符番を付し、その説明は省略することとする。

【００３２】

図５に示されるように、本コンテンツ再生装置２００のＴＲＭ部２１０は、さらに、上記対応表を格納するための対応表格納部２１２を備える。さらにまた、コンテンツ再生装置２００のコンテンツ再生条件管理部２１１は、対応表格納部２１２に格納されている対応表に基づいて、不正なライセンスチケットの上書きを防止する。

また、セキュアフラッシュ部１２０は、新たにＬＴ＿ＩＤとライセンスチケットのアップデート回数との連結データに対するデジタル署名が施されたデータ２２１ｃを格納する。

【００３３】

図６は、上記コンテンツ再生条件管理部２１１の機能構成を表すブロック図である。図６に示されるように、コンテンツ再生条件管理部２１１は、再生状況分析部１１２、全体制御部２１３、暗号化／復号化部１１４及びデジタル署名管理部２１４を備える。

全体制御部２１３は、コンテンツ再生条件管理部２１１の全体を制御する部署であり、例えばＲＯＭやＲＡＭを備えるマイクロコンピュータである。全体制御部２１３は、上記実施の形態１における全体制御部１１３の機能に加え、デジタル署名管理部２１４の制御を行う。さらに、全体制御部２１３は、ＬＴ＿ＩＤとアップデート回数との組の情報（以下「連結情報」という。）を作成して保持する。

【００３４】

デジタル署名管理部２１４は、全体制御部２１３の指示に基づいて、連結情報に対してデジタル署名を施してセキュアフラッシュ部１２０に格納すると共に、セキュアフラッシュ部１２０に格納されている連結情報を読み出して、その正当性を検証する。なお、上記のデジタル署名の施し方及びその検証方法は、従来の技術を使用することとする。

以下、全体制御部２１３が、上記対応表に基づいて古いライセンスチケットの上書きを防止する方法について、以下に示す図７を参照しながら説明する。

【００３５】

図７は、対応表格納部２１２に格納されている対応表の一例である。図７に示されるように、対応表５０には、ＬＴ－ＩＤとアップデート回数とが対応づけられて格納されている。従って、全体制御部２１３が、ライセンスチケット（例えば、「ＡＢＣ＿００１１」というライセンスチケット）についてアップデート回数をインクリメントするように管理すれば、ＴＲＭ部２１０に保持されている連結情報と、セキュアフラッシュ部１２０に格納されている連結情報とを照合することによって、不正に上書きされたか否かを確認することができる。

【００３６】

図８は、本実施の形態におけるコンテンツ再生条件管理部２１１における処理の流れを示すフローチャートである。なお、上記実施の形態１における図３のフローチャートと同一の処理については同一の符番を付し、その説明は省略する。

まず、全体制御部２１３は、上記実施の形態１の場合と同様に、再生指示に係るコンテンツに対応するライセンスチケットの存在を確認し（Ｓ２０３：Ｙｅｓ）、コンテンツ復号部５２０からコンテンツの再生に関する情報を受信すると（Ｓ２０６：Ｙｅｓ）、セキュアフラッシュ部１２０に格納されている、デジタル署名が施されている連結情報を読み出し、ＴＲＭ固有鍵を用いて、その正当性を検証するようにデジタル署名管理部２１４に指示する（Ｓ６０１）。そして、連結情報が正当な場合（Ｓ６０２：Ｙｅｓ）、全体制御部２１３は、ライセンスチケットを復号するように暗号化／復号化部１１４に指示する（

Ｓ２０５）。

【００３７】

さらに、全体制御部２１３は、コンテンツ再生条件情報５１１ａを含むＬＴの内容を更新して、再び上記ＴＲＭ固有鍵を用いて暗号化するように暗号化／復号化部１１４に指示する（Ｓ２０６）。さらにまた、全体制御部２１３は、アップデート回数をインクリメントすると共に（Ｓ６０３）、連結情報にデジタル署名を施すようにデジタル署名管理部２１４に指示する（Ｓ６０４）。そして、暗号化されたＬＴ及び上記デジタル署名が施された連結情報をセキュアフラッシュ部１２０に書き込むように、暗号化／復号化部１１４及びデジタル署名管理部２１４に指示する（Ｓ６０５）。

【００３８】

なお、上記の実施の形態２では、ＬＴ＿ＩＤに対応付ける情報としてアップデート回数を挙げて説明したが、アップデート回数に限らず、アップデートを行った事実を識別することが可能な乱数等の情報であってもよい。

また、上記の実施の形態２では、対応表はＴＲＭ部で保持する実施例について説明したが、対応表もセキュアフラッシュ部に格納し、対応表のハッシュ値をＴＲＭ部で保持することとしてもよい。さらにまた、ライセンスチケット毎のデジタル署名又はハッシュ値をセキュアフラッシュ部に格納し、それらのハッシュ値をＴＲＭ部で保持することとしてもよい。なお、ライセンスチケットのコンテンツ再生条件情報の中で更新する必要のない再生条件（例えば、再生可能な有効期限など）については、対応表に記載させないこととし、その分メモリ容量の軽減を図ってもよい。

【００３９】

以上のように、本実施の形態におけるコンテンツ再生装置によれば、ライセンスチケットをセキュアフラッシュ部に格納すると共に、ライセンスチケットを識別し得る情報（ＬＴ＿ＩＤ）とアップデート回数とが対応付けられている対応表に基づいてライセンスチケットの正当性も検証するので、ＴＲＭ部の記憶容量を最小限に抑えると共に、より安全性を高めてライセンスチケットを管理することが可能となる。

【００４０】

また、上記の実施の形態１及び実施の形態２では、コンテンツ復号部は、ＴＲＭ部の外部に備えるように構成したが、ＴＲＭ部の内部に備えることとしてもよい。

【産業上の利用可能性】

【００４１】

本発明に係るライセンス情報管理装置及びライセンス情報管理方法は、著作権の保護を必要とする暗号化されたコンテンツの再生を可能とするＤＶＤ再生装置等のパッケージコンテンツの再生装置やネットワークを介して暗号化されたコンテンツを受信して再生するパーソナルコンピュータ等に利用が可能である。

【図面の簡単な説明】

【００４２】

【図１】実施の形態１に係るコンテンツ再生装置の機能構成を示すブロック図である。

【図２】実施の形態１におけるコンテンツ再生条件管理部の機能構成を示すブロック図である。

【図３】実施の形態１におけるコンテンツ再生条件管理部の処理の流れを示すフローチャートである。

【図４】実施の形態１に係るコンテンツ再生装置の課題を説明するための図である。

【図５】実施の形態２に係るコンテンツ再生装置の機能構成を示すブロック図である。

【図６】実施の形態２におけるコンテンツ再生条件管理部の機能構成を示すブロック図である。

【図７】実施の形態２における対応表の一例を示す図である。

【図８】実施の形態２におけるコンテンツ再生条件管理部の処理の流れを示すフロー

チャートである。

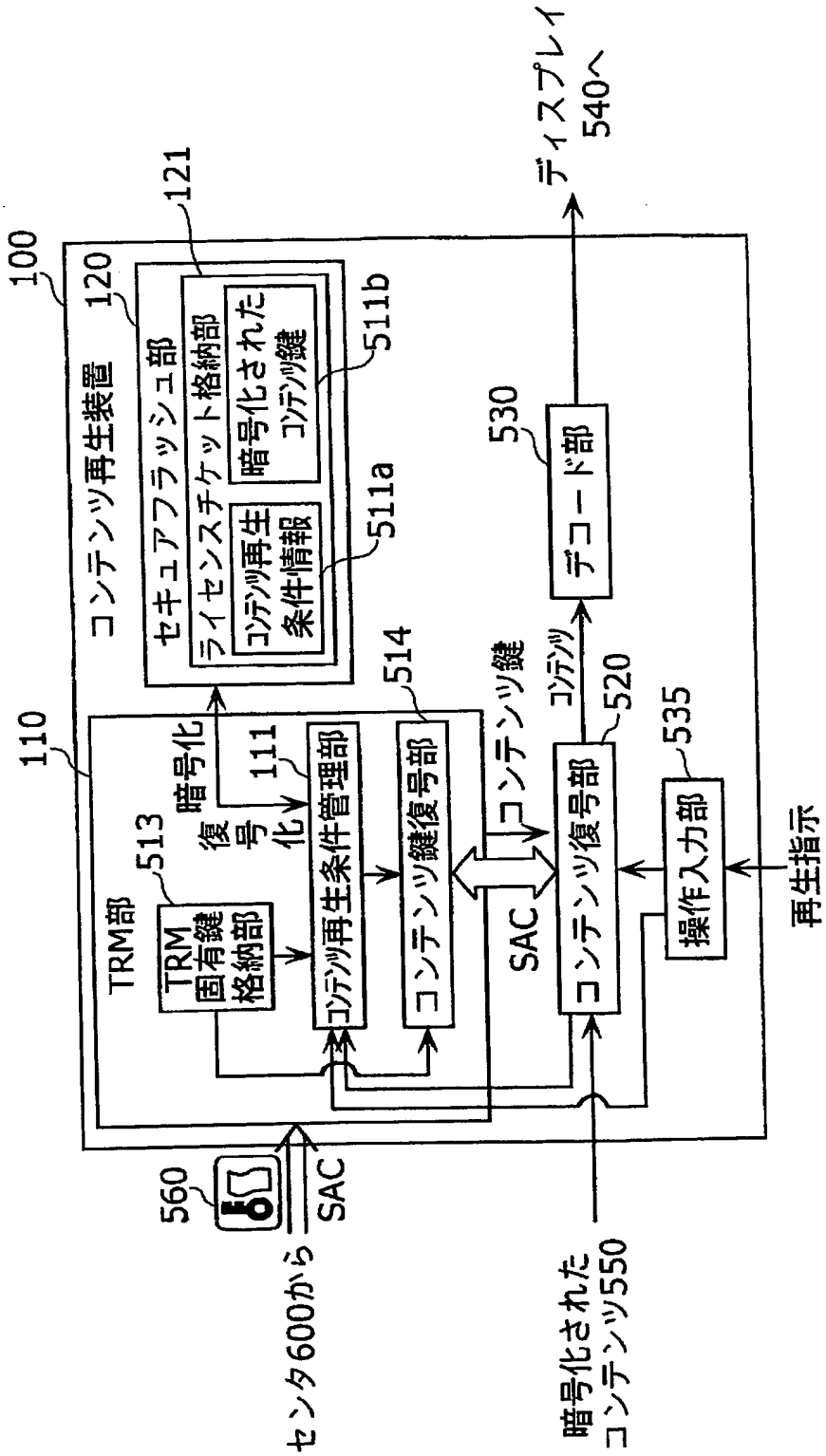
【図９】従来の技術に係るコンテンツ再生装置の機能構成を示すブロック図である。

【符号の説明】

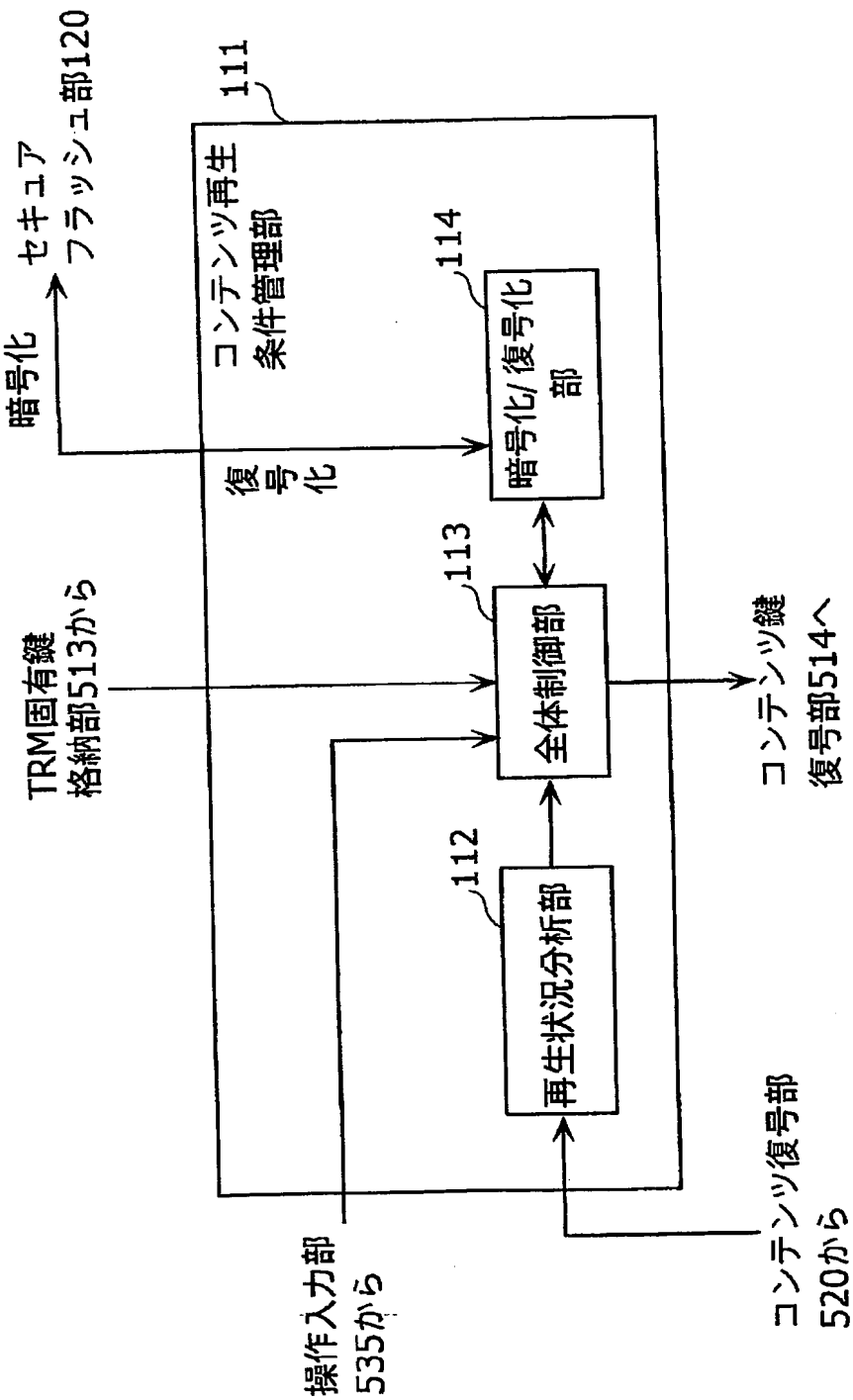
【００４３】

５０	対応表
１００、２００、５００	コンテンツ再生装置
１１０、２１０、５１０	ＴＲＭ部
１１１、２１１、５１２	コンテンツ再生条件管理部
１１２	再生状況分析部
１１３、２１３	全体制御部
１１４	暗号化／復号化部
１２０	セキュアフラッシュ部
１２１	ライセンスチケット格納部
２１２	対応表格納部
２１４	デジタル署名管理部
５１１ａ	コンテンツ再生条件情報
５１１ｂ	暗号化されたコンテンツ鍵
５１３	ＴＲＭ固有鍵格納部
５１４	コンテンツ鍵復号部
５２０	コンテンツ復号部
５３０	デコード部
５３５	操作入力部
５４０	ディスプレイ
５５０	暗号化されたコンテンツ
５６０	ライセンスチケット
６００	センタ

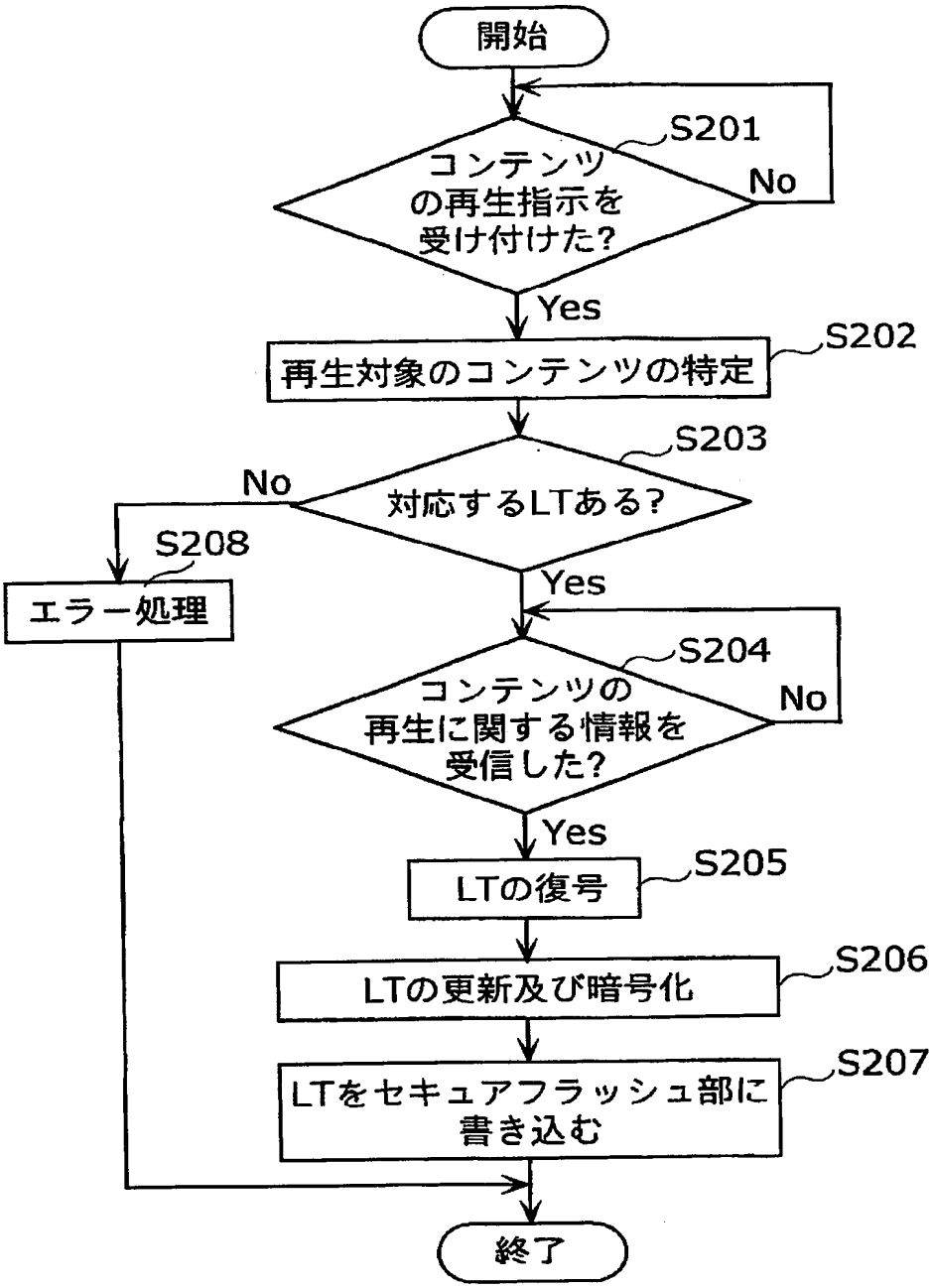
【書類名】図面
【図１】


100
コンテンツ再生装置
120
121
セキュアフラッシュ部
ライセンスチケット格納部
コンテンツ再生条件情報
511a
暗号化されたコンテンツ鍵
511b
ディスプレイ540へ
530
デコード部
110
暗号化
復号化
111
514
コンテンツ鍵復号部
コンテンツ鍵
コンテンツ
520
535
TRM部
513
TRM固有鍵格納部
コンテンツ再生条件管理部
SAC
コンテンツ復号部
操作入力部
再生指示
560
SAC
センタ600から
暗号化されたコンテンツ550

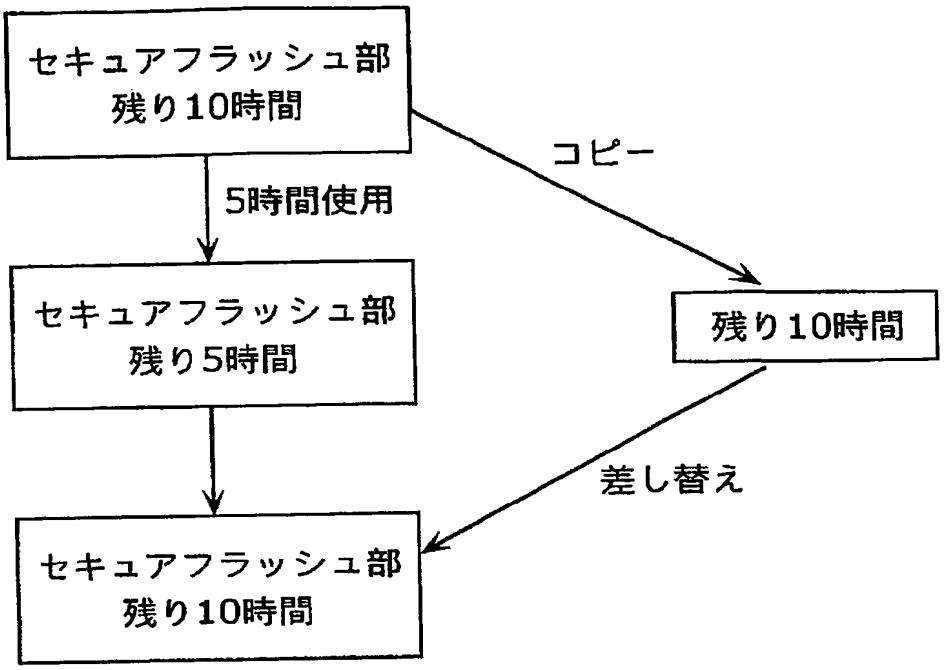
【図２】


111
コンテンツ再生
条件管理部
114
暗号化/復号化
部
113
全体制御部
112
再生状況分析部
暗号化
セキュア
フラッシュ部120
復号化
TRM固有鍵
格納部513から
コンテンツ鍵
復号部514へ
操作入力部
535から
コンテンツ復号部
520から

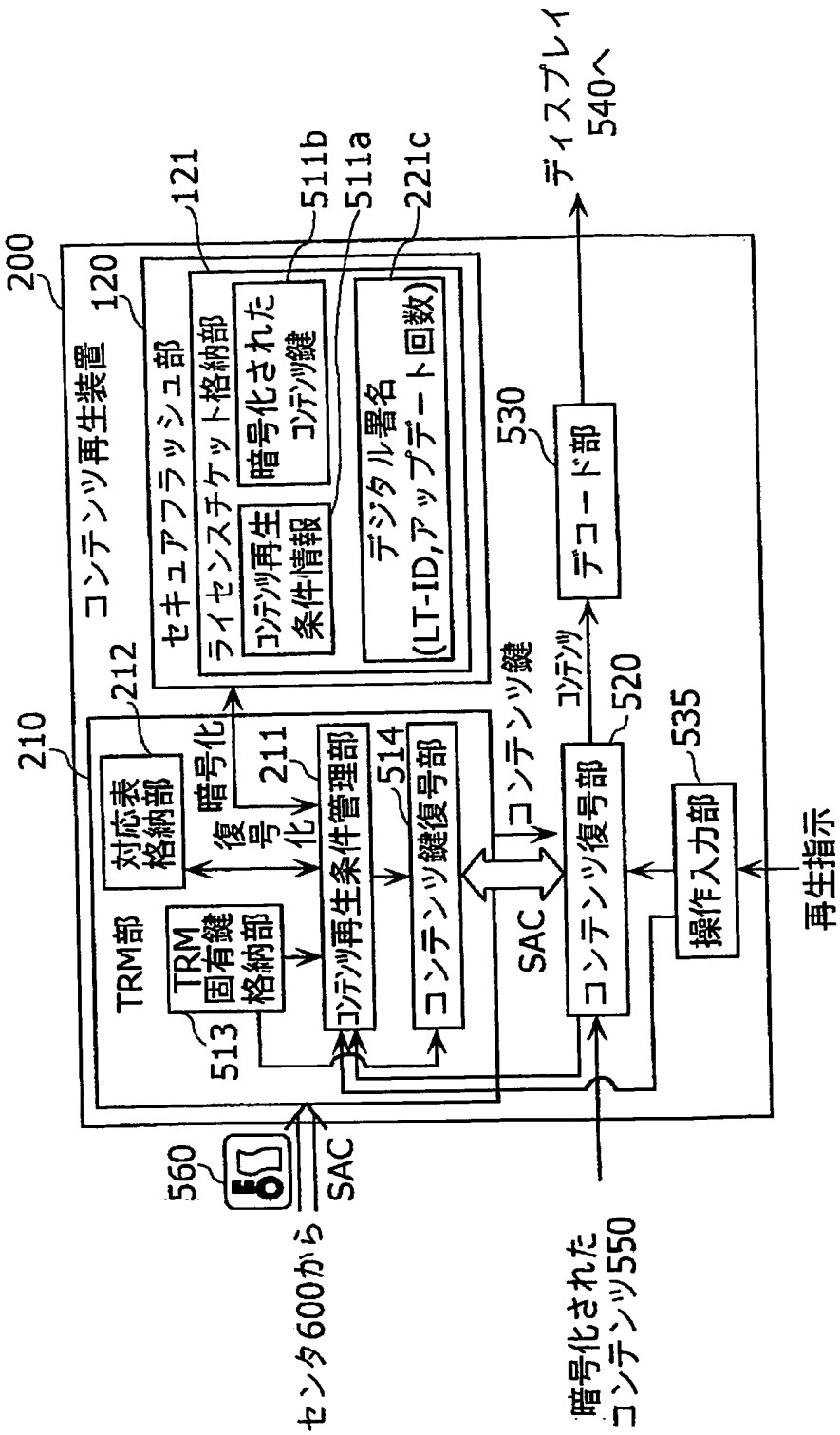
【図３】


開始
S201
コンテンツの再生指示を受け付けた?
No
Yes
S202
再生対象のコンテンツの特定
S203
対応するLTある?
No
Yes
S208
エラー処理
S204
コンテンツの再生に関する情報を受信した?
No
Yes
S205
LTの復号
S206
LTの更新及び暗号化
S207
LTをセキュアフラッシュ部に書き込む
終了

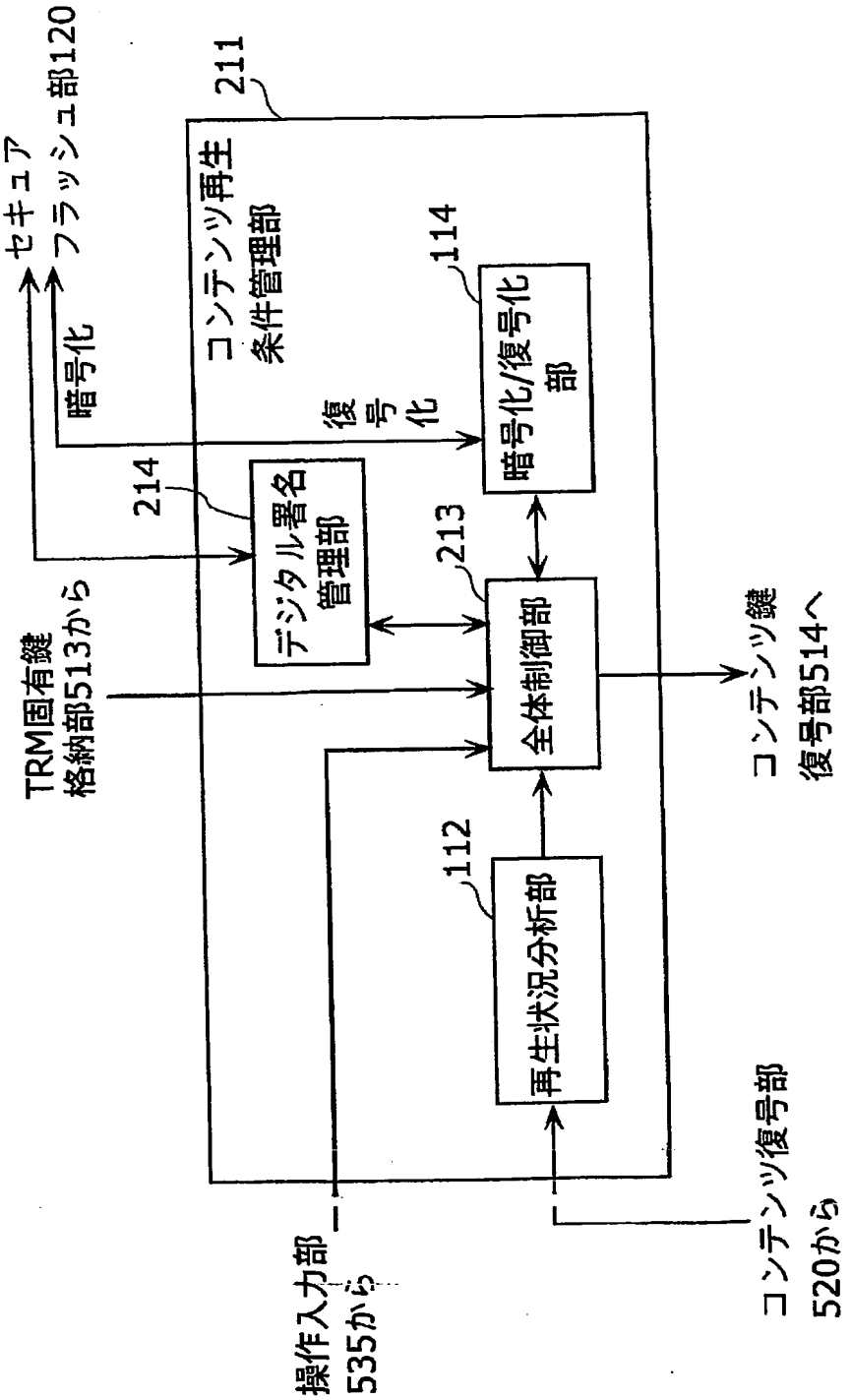
【図４】


セキュアフラッシュ部
残り10時間
5時間使用
コピー
セキュアフラッシュ部
残り5時間
残り10時間
差し替え
セキュアフラッシュ部
残り10時間

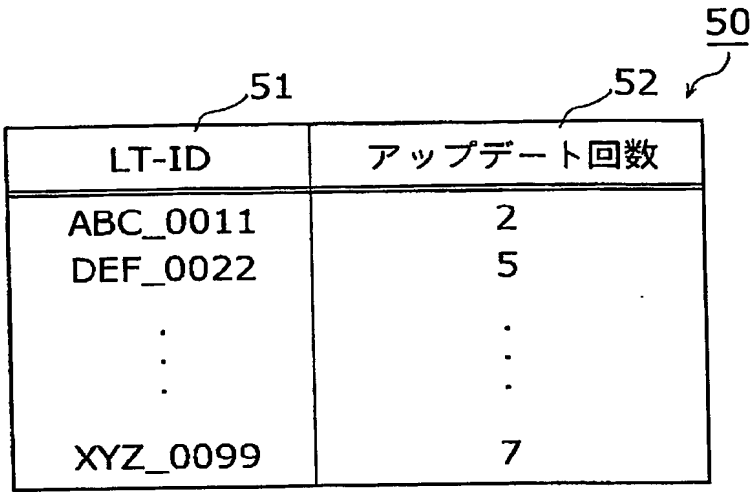
【図５】


200
コンテンツ再生装置
120
121
セキュアフラッシュ部
ライセンスチケット格納部
511b
511a
221c
暗号化された
コンテンツ鍵
コンテンツ再生
条件情報
デジタル署名
(LT-ID,アップデート回数)
ディスプレイ
540へ
530
デコード部
コンテンツ
520
535
210
212
対応表
格納部
暗号化
復号化
211
514
コンテンツ再生条件管理部
コンテンツ鍵復号部
コンテンツ鍵
SAC
コンテンツ復号部
操作入力部
再生指示
TRM部
TRM
固有鍵
格納部
513
560
SAC
センタ600から
暗号化された
コンテンツ550

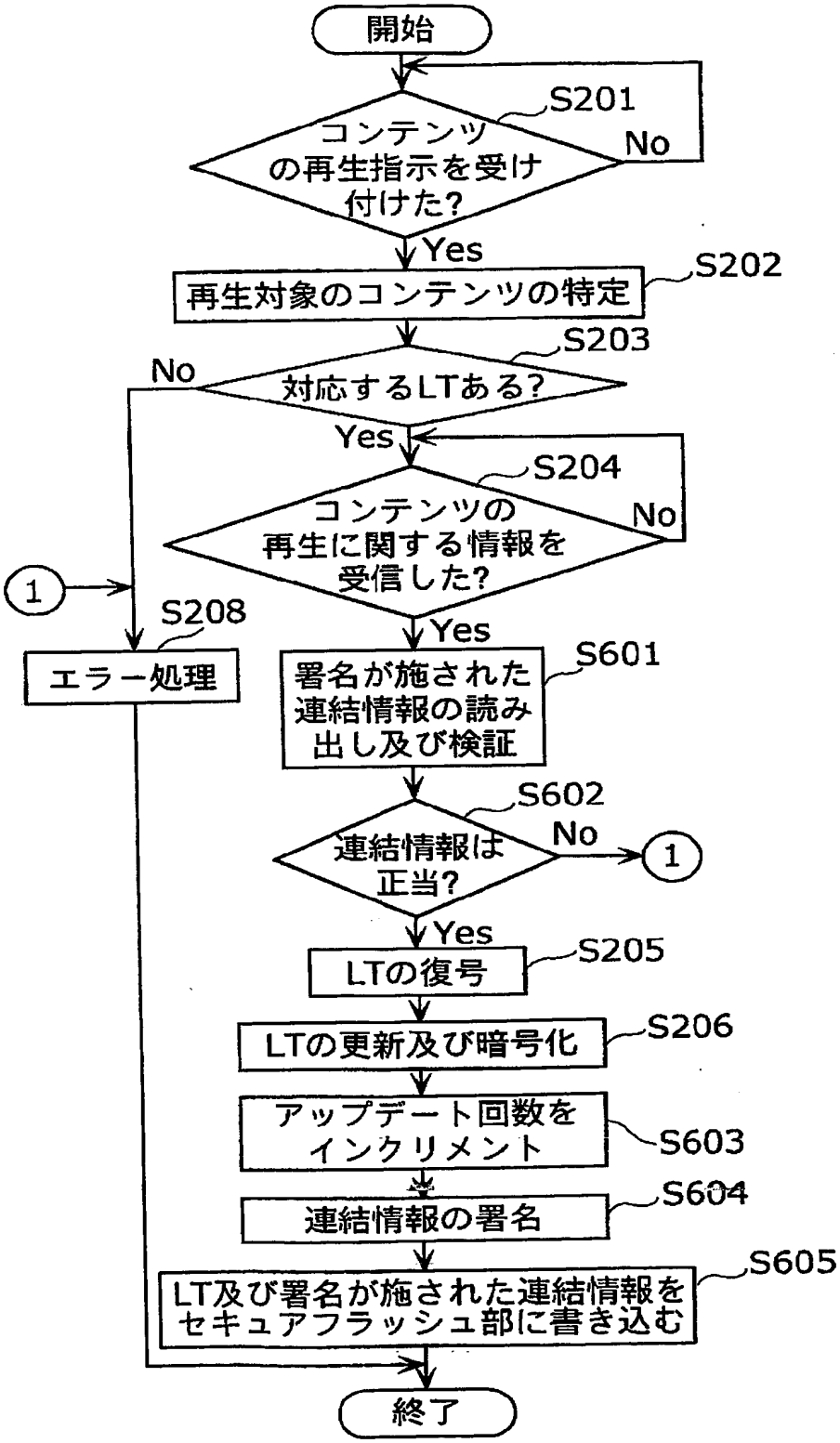
【図６】


セキュア
フラッシュ部120
211
コンテンツ再生
条件管理部
暗号化
復号化
114
暗号化/復号化
部
214
デジタル署名
管理部
213
TRM固有鍵
格納部513から
全体制御部
コンテンツ鍵
復号部514へ
112
再生状況分析部
操作入力部
535から
コンテンツ復号部
520から

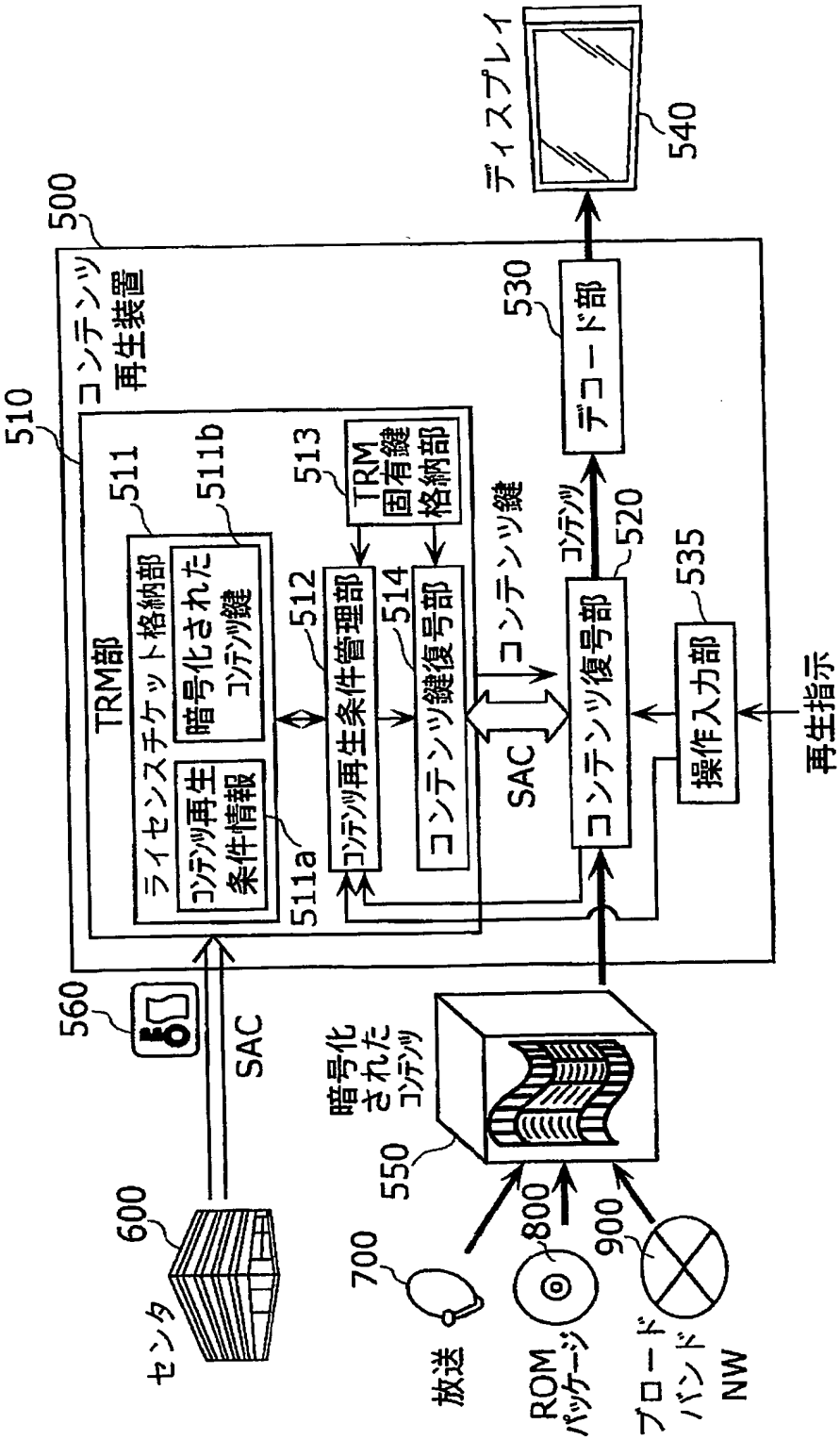
【図７】



【図８】


開始
S201
コンテンツの再生指示を受け付けた?
No
Yes
S202
再生対象のコンテンツの特定
S203
対応するLTある?
No
Yes
S204
コンテンツの再生に関する情報を受信した?
No
Yes
1
S208
エラー処理
S601
署名が施された連結情報の読み出し及び検証
S602
連結情報は正当?
No
1
Yes
S205
LTの復号
S206
LTの更新及び暗号化
S603
アップデート回数をインクリメント
S604
連結情報の署名
S605
LT及び署名が施された連結情報をセキュアフラッシュ部に書き込む
終了

【図９】


ディスプレイ
540
500
コンテンツ
再生装置
530
デコード部
510
TRM部
511
ライセンスチケット格納部
コンテンツ再生
条件情報
511a
511b
暗号化された
コンテンツ鍵
513
TRM
固有鍵
格納部
512
コンテンツ再生条件管理部
514
コンテンツ鍵復号部
コンテンツ鍵
SAC
コンテンツ
520
コンテンツ復号部
535
操作入力部
再生指示
560
SAC
暗号化
された
コンテンツ
550
600
センタ
700
放送
800
ROM
パッケージ
900
ブロード
バンド
NW

【書類名】要約書
【要約】
【課題】　ユーザが多数のコンテンツを所有する場合であっても、大容量の耐タンパモジュールが必要とならないライセンス情報管理装置等を提供する。
【解決手段】　全体制御部１１３は、ユーザから受信した再生指示に対応するコンテンツを特定する（Ｓ２０２）。全体制御部１１３は、特定されたコンテンツに対応するＬＴが、セキュアフラッシュ部１２０にＬＴが存在するか否かを確認する。セキュアフラッシュ部１２０にＬＴが存在し（Ｓ２０３：Ｙｅｓ）、コンテンツ復号部５２０からコンテンツの再生に関する情報を受信すると（Ｓ２０４：Ｙｅｓ）、暗号化／復号化部１１４は、ＴＲＭ固有鍵を用いてセキュアフラッシュ部１２０に格納されているＬＴを復号する（Ｓ２０５）。その後、暗号化／復号化部１１４は、コンテンツ再生条件情報５１１ａの内容を更新して、ＴＲＭ固有鍵を用いて暗号化して（Ｓ２０７）、これをセキュアフラッシュ部１２０に書き込む（Ｓ２０８）。
【選択図】　図３

認定・付加情報

特許出願の番号	特願２００４－０３２６７６
受付番号	５０４００２１１２９４
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１６年　２月１０日

＜認定情報・付加情報＞

【提出日】　平成16年 2月 9日

特願２００４－０３２６７６

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002110

International filing date: 04 February 2005 (04.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-032676
Filing date: 09 February 2004 (09.02.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse